Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Corporate Perspectives On Cybersecurity: A Survey Of Execs

Law360, Washington (May 06, 2015, 11:16 AM ET) --

Marcus Christian

In an effort to gauge industry concerns and measure corporate responses to significant privacy and security threats, my firm, Mayer Brown LLP, conducted an informal survey of key executives and corporate counsel in 15 industry sectors between mid-November 2014 and mid-February 2015. The majority of the companies were from finance and financial institutions, professional services (law, medicine, accounting, architecture and design), utilities and energy (including extraction), health care and pharmaceuticals. While two-thirds (70 percent) of the respondents' companies have a chief information officer or both a CIO and a chief privacy officer, one-fifth (21 percent) of the companies had neither.

Survey Summary

Survey respondents overwhelmingly considered the disclosure of personally, identifiable information as the biggest cyber-related threat to their companies (63 percent). Concern about interruption of business operations such as system sabotage ranked second (24 percent). Less than 10 percent of the respondents considered theft of trade secrets as the most serious threat. Most respondents (63 percent) considered cyber issues to be just one more cost of doing business or that these problems can be overcome. Well over half (57 percent) of the respondents estimated that litigation risk posed by cybersecurity issues has a relatively modest impact on their cybersecurity planning. For some, pessimism reigns. Around 29 percent of respondents have a negative outlook on cyber-related issues, believing that cybercrime will always be one step ahead of legislative protections and enforcement.

The survey revealed that respondents' concern about the adverse impact of regulatory enforcement appreciably affects their willingness to share incident information with the government. Liability protection is a critical component of a voluntary cyber information-sharing program. Without meaningful liability protection, companies will be hesitant to participate because any act or omission made by a participant based upon cyberthreat information received by that entity could subject it to liability. This concern may also explain why only 23 percent of respondents said that their company had built a close working relationship with either a government enforcement agency (FBI, U.S. Secret Service) or a prosecutorial agency (U.S. Department of Justice or state attorneys general) on cyber issues. An equivalent percentage (23 percent) reported working closely with industry regulatory (Federal

Trade Commission, Federal Communications Commission, Federal Deposit Insurance Corporation, Consumer Financial Protection Bureau). Over 40 percent said, “no, they have no such relationship,” while approximately 24 percent did not know.

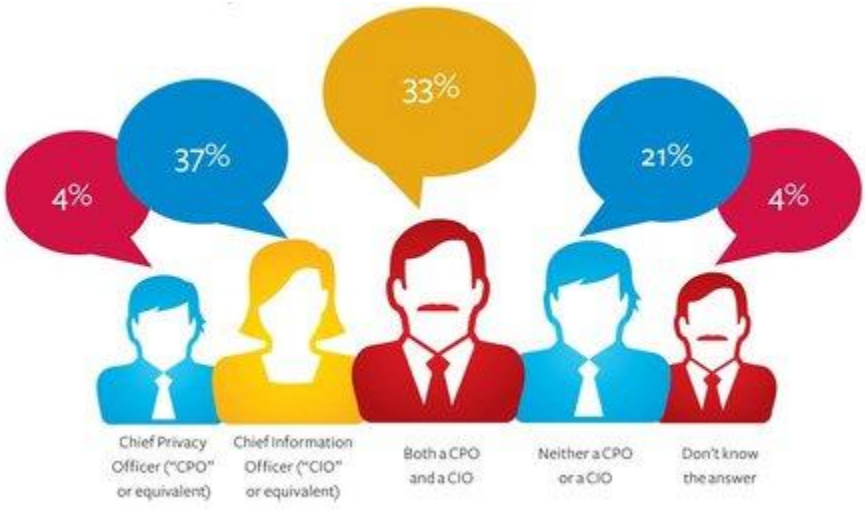
The survey showed that 84 percent of respondents expect clear national standards on data breach notification to emerge within the next five years. Smaller numbers expected national standards for securing personally identifiable information, investor disclosures and liability protection for information-sharing.

This may reflect a growing recognition in Congress that having 47 different reporting standards does not make sense. Given the number of breaches that have occurred in recent years, it makes sense to instead have a clear set of standards, not just for notification but for information security as well.

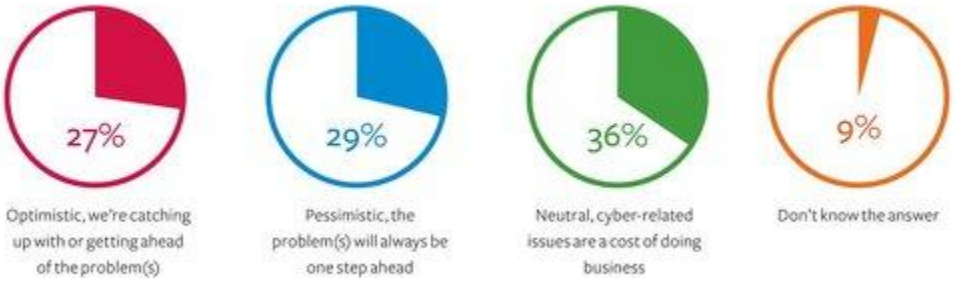
Nearly 50 percent of respondents weren’t sure if the National Institute of Standards and Technology Cybersecurity Framework has been helpful to their company in managing cybersecurity risk. This may indicate that it is premature to judge the NIST framework, or that companies are not sufficiently aware of how it is meant to be helpful.

Full Survey Results

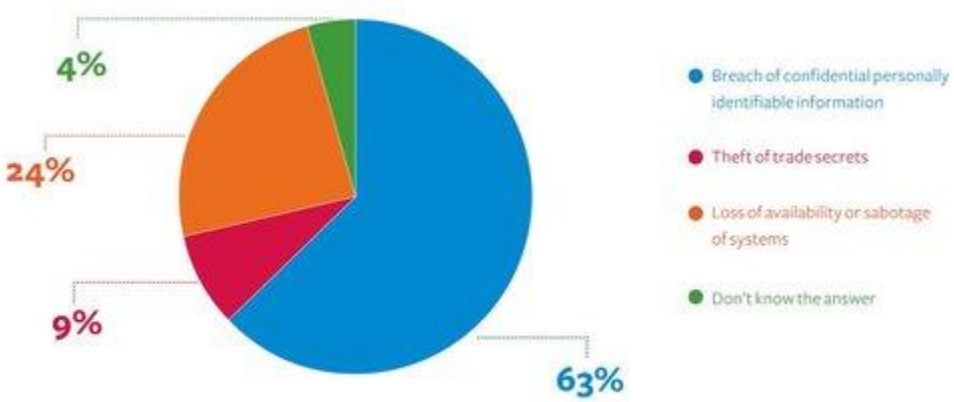
1. Does your organization have a chief privacy officer or a chief information officer who is accountable for developing, implementing and maintaining an organization-wide governance and privacy/cybersecurity program?



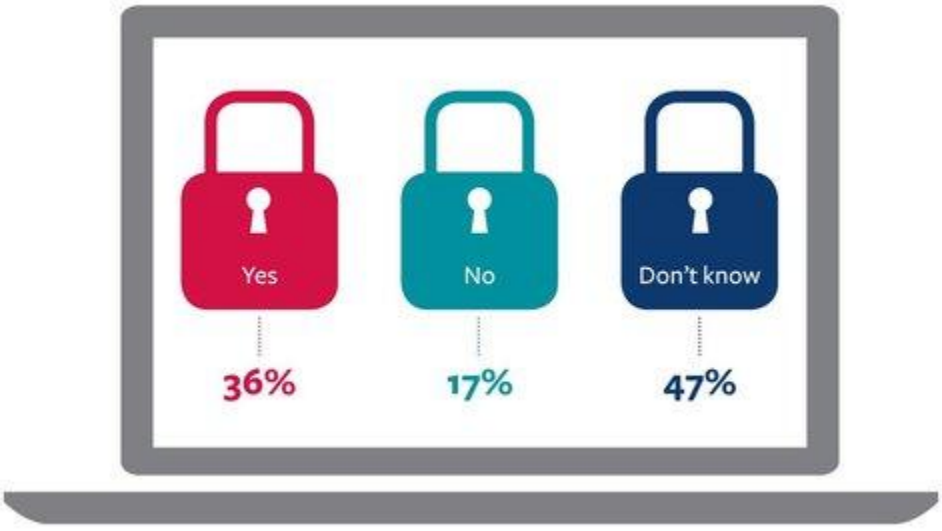
2. How would you describe your outlook on cybersecurity issues? For this survey, “cybersecurity issues” could include breaches, attacks, denial of service, loss of data, and/or damage to cyber infrastructure.



3. Which do you consider the biggest threat to your company?

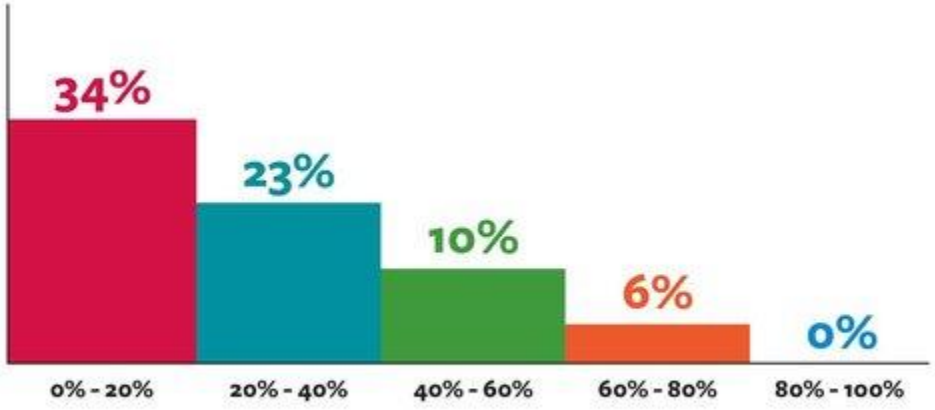


4. Has the NIST Cybersecurity Framework been helpful to your company in managing cybersecurity risk?



5. Has your company built a close working relationship with a government entity on cybersecurity issues (more than one answer could have been selected)?

6. Which of the following percentage ranges best represents the estimated amount that litigation risk associated with cybersecurity issues influences your company's cybersecurity planning?



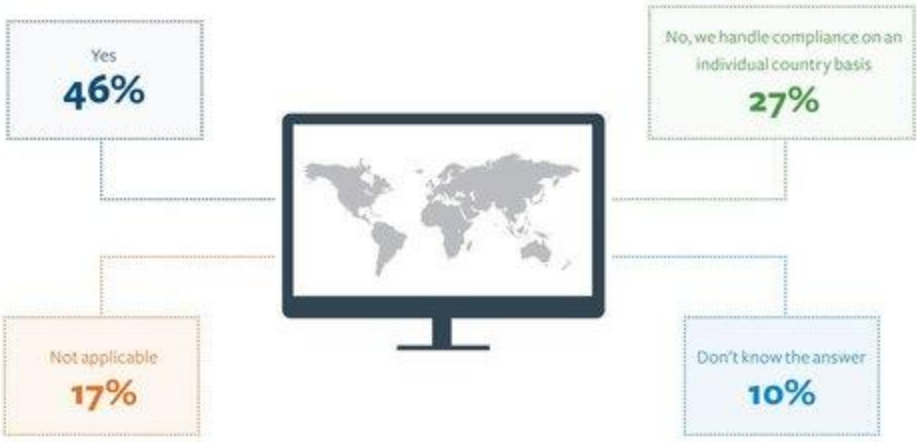
*Don't know the answer - 27%

7. Does concern about regulatory enforcement actions or other adverse regulatory action impact your company's willingness to share incident information with the government?

*Don't know the answer - 30%

8. Do you expect clear national standards to emerge in the next five years in the following areas (more than one answer could have been selected)?

9. Has your company developed a global strategy to meet the differing cybersecurity and data privacy legal requirements of the countries in which you operate?



10. Does your company have a separate cyberinsurance policy?

*Don't know the answer - 33%

11. Does your organization have a written data protection plan? If so, how was the plan prepared (more than one answer could have been selected)?

12. If your company suspected that a cyber-related incident had occurred, which two external entities on the following list do you believe your company would contact first?

*Don't know the answer **8%**

Discussion

The above survey includes several questions about corporate engagement with government agencies to promote cybersecurity. Respondents' answers to those questions suggest that a considerable number of businesses remain wary of collaborating with government agencies. These responses are noteworthy because such efforts — particularly public-private information-sharing initiatives — form a critical part of the United States' strategy against cybercrime and cyberespionage.[1] Such efforts generally enjoy bipartisan support and broad recognition as best practices. But to work optimally, these initiatives also must gain widespread and committed business participation. That is no small task. It requires policymakers and others to understand and address the private sector's reluctance to collaborate with government entities.

For years, partnerships between government and private entities have been central in the United States' cybersecurity policy. This approach rests upon notions that "[i]ndustry and governments share the responsibility for the security and reliability of the infrastructure and the transactions that take place on it and should work closely together to address these interdependencies" and that "[p]rivate-sector engagement is required to help address the limitations of law enforcement and national security."[2] Information-sharing partnerships are viewed as essential.[3] The logic behind them is straightforward. By participating in cyber information-sharing programs, companies can gain early knowledge of emerging threats and effective defenses. This timely information enhances businesses' abilities to prevent, detect and respond to cyber intrusions. Information-sharing may occur over computer networks, through written communications, and in conversations, among other means.

In part, the survey shows that most participants' companies currently lack close working relationships with law enforcement on cybersecurity issues and worry that sharing protected information with other organizations could trigger regulatory scrutiny. Specifically, when asked whether concerns about enforcement actions affect their companies' willingness to share cyberincident information with the government, more than 60 percent of the individuals who rated their companies indicated that the possibility of regulatory enforcement actions has a moderate or greater effect on their willingness to share information.[4]

Moreover, in response to a question about interactions with law enforcement agencies, only one in five survey respondents reported that their company had developed a close working relationship with a law enforcement agency such as the FBI or the Secret Service.[5] Businesses primarily interact with the FBI through its Infragard chapters and Cyber Task Forces. And the Secret Service regularly engages with members of the private sector through its Electronic Crimes Task Forces.

Participants also were asked whether they expect a "clear national standard" to emerge over the next five years for data breach notification, security of personally identifiable information, or liability protection for information sharing (among other areas). Only 30 percent of respondents indicated that they expect that Congress or another body will create a standard to protect companies sharing threat information from liability. In contrast, 84 percent of the respondents expect a data breach notification standard, and 54 percent expect standards for the security of personally identifiable information.

A national standard for information-sharing liability protection may emerge in the near future. Recently, the U.S. House of Representatives passed H.R. 1560, the Protecting Cyber Networks Act, and H.R. 1731, the National Cybersecurity Protection Advancement Act. The companion, bipartisan bills were drafted to provide a legal framework for voluntary cyber information-sharing among governments and private

entities. If enacted, the measures will expand private sector participants' real-time access to information, including classified information. In addition, the bills include provisions to shield participating companies from lawsuits and regulatory enforcement actions related to their good faith efforts to share threat information and protect civil liberties. To the extent that the type of liability protections included in H.R. 1560 and H.R. 1731 adequately address organizations' concerns about civil and regulatory liability, they are a necessary part of an information-sharing framework.

But only time will tell whether such protections will be sufficient to gain widespread private-sector participation in threat-sharing programs. Additional obstacles remain. Participating in information-sharing programs is not free. It requires an investment of human and financial capital. To become eligible to receive all available information, businesses will need to satisfy many requirements, including gaining necessary security clearances for employees, installing systems to store and transmit classified information, and managing access to threat information. Companies also may need to make significant expenditures to buy systems and software to become compatible with information-sharing platforms and to develop expertise and processes to remove customers' personally identifiable information from information they share. Depending upon the volume of information they receive, businesses may require additional personnel to analyze threat information.

In addition, many organizations fear that other entities will disclose their breaches and other computer security incidents to the public. When a company shares threat information, a virtually limitless number of entities, including government agencies, insurers, competitors and security companies might receive it. Because threat information can contain data about its victims, sharing it can reveal that a specific company has suffered a breach or other computer security incident. In general, as the number of entities that know about a breach increases, so does the likelihood that it will become public. For many companies, this potential cost outweighs any anticipated benefits.

Other businesses, particularly those seeking to brand themselves as defenders of civil liberties, will seek to avoid a backlash over civil liberties concerns. Several advocacy organizations have criticized information-sharing legislation as blueprints for surveillance programs that will impact law-abiding citizens more than cybercriminals and other threat actors. Although H.R. 1560 and H.R. 1731 each include explicit protections for civil rights, critics have dismissed these proposed protections as inadequate. If large numbers of consumers begin to express disapproval of information-sharing efforts, some businesses will delay or cancel plans to join threat sharing initiatives.

Even without a consumer backlash, many companies will take a wait-and-see approach. Although organizations might be able to predict their startup costs for joining information-sharing programs, insufficient data currently exist to make reasonable estimations of the benefits. The government will gain from monitoring the impact of information-sharing efforts and disclosing the results to potential participants. Given the growing pains that new initiatives normally experience, a significant number of organizations likely will examine impact data before joining an initiative.

If Congress enacts an information-sharing law in the near future, agencies tasked with implementing it will profit from paying attention to companies' concerns. Several elements of the survey revealed a hesitance to work with the government on cybersecurity. To overcome private sector wariness, the government will need to understand the full spectrum of factors likely to influence businesses' decisions to join the initiative. Then it will need to make a compelling business case for why individual companies should participate.

—By Marcus Christian, Mayer Brown LLP

Marcus Christian is a partner in Mayer Brown's Washington, D.C., office and former executive assistant U.S. attorney at the U.S. Attorney's Office for the Southern District of Florida.

[1] See Executive Order No. 13636, 3 C.F.R. 33 (2013).

[2] See Cyberspace Policy Review: Assuring a Trusted and Resilient Information

and Communications Infrastructure 17-29 (2010), available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[3] See Executive Order: Promoting Private Sector Cybersecurity Information Sharing (Feb. 13, 2015), available at https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[4] Thirty percent of the respondents indicated that they did not know the answer to the question.

[5] In addition, 23 percent of respondents reported that their companies had developed a working relationship with the Federal Trade Commission, Federal Communications Commission, the Federal Deposit Insurance Corporation, or other industry regulator. Forty-one percent of respondents answered that their companies have not developed a close working relationship with a government entity on cybersecurity issues.
